

Department of Energy

§ 1045.20

Top Secret if it is vital to the national security and if its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of RD information that warrant Top Secret classification include detailed technical descriptions of critical features of a nuclear explosive design that would enable a proliferant or nuclear power to build or substantially improve a nuclear weapon, information that would make possible the unauthorized use of a U.S. nuclear weapon, or information revealing catastrophic failure or operational vulnerability in a U.S. nuclear weapon.

(2) *Secret*. The Director of Classification shall classify RD information as Secret if its unauthorized disclosure could reasonably be expected to cause serious damage to the national security, but the RD information is not sufficiently comprehensive to warrant designation as Top Secret. Examples of RD information that warrant Secret classification include designs for specific weapon components (not revealing critical features), key features of uranium enrichment technologies, or specifications of weapon materials.

(3) *Confidential*. The Director of Classification shall classify RD information as Confidential if it is deemed to be of significant use to a potential adversary or nuclear proliferant and its unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security. Examples of RD information that warrant Confidential classification are the amount of high explosives used in nuclear weapons, gaseous diffusion design information, and design information for Naval reactors.

(b) *Formerly Restricted Data*. The Director of Classification, jointly with the DoD, shall assign one of the classification levels in paragraph (a) of this section to FRD information to reflect its sensitivity to the national security.

[62 FR 68509, Dec. 31, 1997, as amended at 71 FR 68737, Nov. 28, 2006]

§ 1045.18 Newly generated information in a previously declassified subject area.

(a) The Director of Classification may evaluate newly generated specific

information in a previously declassified subject area using the criteria in section 1045.16 and classify it as RD, if warranted.

(b) The Director of Classification shall not classify the information in such cases if it is widely disseminated in the public domain.

[62 FR 68509, Dec. 31, 1997, as amended at 71 FR 68737, Nov. 28, 2006]

§ 1045.19 Accountability for classification and declassification determinations.

(a) Whenever a classification or declassification determination concerning RD or FRD information is made, the Director of Classification and the Chief Health, Safety and Security Officer shall be able to justify the determination. For FRD and RD primarily related to military utilization, the Director of Classification and the Chief Health, Safety and Security Officer shall coordinate the determination and justification with the DoD. If the determination involves a departure from the presumptions in § 1045.15, the justification shall include a rationale for the departure. Often the justification itself will contain RD or FRD information. In such a case, the Director of Classification and the Chief Health, Safety and Security Officer shall ensure that a separate justification can be prepared which is publicly releasable. The publicly releasable justification shall be made available to any interested person upon request to the Director of Classification.

(b) The Director of Classification shall prepare a report on an annual basis on the implementation of this part. This report shall be available to any interested person upon request to the Director of Classification. Requests may be submitted to the Director Office of Classification, HS-90/Germantown Building, U.S. Department of Energy, 1000 Independence Avenue SW., Washington, DC 20585-1290.

[62 FR 68509, Dec. 31, 1997, as amended at 71 FR 68737, Nov. 28, 2006]

§ 1045.20 Ongoing call for declassification proposals.

The Chief Health, Safety and Security Officer shall consider proposals

§ 1045.21

from the public or agencies or contractors for declassification of RD and FRD information on an ongoing basis. Declassification proposals for RD and FRD information shall be forwarded to the Chief Health, Safety and Security Officer, HS-1/Forrestal Building, U.S. Department of Energy, 1000 Independence Avenue SW, Washington, DC 20585. Any proposed action shall include a description of the information concerned and may include a reason for the request. DOE and DoD shall coordinate with one another concerning declassification proposals for FRD information.

[62 FR 68509, Dec. 31, 1997, as amended at 71 FR 68737, Nov. 28, 2006]

§ 1045.21 Privately generated restricted data.

(a) DOE may classify RD which is privately generated by persons not pursuant to Government contracts, in accordance with the Atomic Energy Act.

(b) In order for information privately generated by persons to be classified as RD, the Secretary or Deputy Secretary shall make the determination personally and in writing. This authority shall not be delegated.

(c) DOE shall publish a FEDERAL REGISTER notice when privately generated information is classified as RD, and shall ensure that the content of the notice is consistent with protecting the national security and the interests of the private party.

§ 1045.22 No comment policy.

(a) Authorized holders of RD and FRD shall not confirm or expand upon the classification status or technical accuracy of classified information in the public domain.

(b) Unauthorized disclosure of classified information does not automatically result in the declassification of that information.

(c) If the disclosure of classified information is sufficiently authoritative or credible, the Chief Health, Safety and Security Officer shall examine the possibility of declassification.

[62 FR 68509, Dec. 31, 1997, as amended at 71 FR 68737, Nov. 28, 2006]

10 CFR Ch. X (1–1–09 Edition)

Subpart C—Generation and Review of Documents Containing Restricted Data and Formerly Restricted Data

§ 1045.30 Purpose and scope.

This subpart specifies Government-wide classification program implementation requirements for agencies with access to RD and FRD, describes authorities and procedures for RD and FRD document classification and declassification, provides for periodic or systematic review of RD and FRD documents, and describes procedures for the mandatory review of RD and FRD documents. This subpart applies to all RD and FRD documents, regardless of whether they also contain National Security Information (NSI), or other controlled information such as “For Official Use Only” information or “Unclassified Controlled Nuclear Information.”

§ 1045.31 Applicability.

This subpart applies to—

(a) Any person with authorized access to RD or FRD;

(b) Any agency with access to RD or FRD; and

(c) Any person generating a document containing RD or FRD.

§ 1045.32 Authorities.

(a) *Classification of RD and FRD documents.* (1) To the maximum extent practical, all RD and FRD documents shall be classified based on joint DOE-Agency classification guides or Agency guides coordinated with the DOE. When it is not practical to use classification guides, source documents may be used as an alternative.

(2) Only individuals designated as RD classifiers may classify RD and FRD documents, except within the DoD. Within the DoD, any individual with access to RD and FRD who has been trained may classify RD and FRD documents.

(3) RD classifiers shall classify only documents in subject areas in which they have programmatic expertise.

(4) RD classifiers may upgrade or downgrade the classification level of RD or FRD documents in accordance with joint DOE-Agency classification